Gemeente Echt-Susteren

GEMEENTEBLAD

Officiële uitgave van gemeente Echt-Susteren.

Nr. 56582

25 juni

2015

Nota Privacybeleid Gemeente Echt-Susteren 2015

1. Inleiding

De gemeente heeft er per 1 januari 2015 taken bijgekregen. Dat komt door de decentralisatie van de Jeugdwet, Wmo 2015 en de Participatiewet. Daardoor heeft de gemeente een nog belangrijkere verantwoordelijkheid gekregen waar het gaat om de verwerking van persoonsgegevens van inwoners. Immers: de gemeente wisselt voortaan nog vaker dan voorheen persoonsgegevens uit met instanties buiten de gemeentelijke organisatie. Ook is de bescherming van persoonlijke gegevens complexer geworden.

De gemeente verzamelt en bewerkt persoonsgegevens voor de dienstverlening aan inwoners en bedrijven. Het gaat bijvoorbeeld om de gegevens in de gemeentelijke basisregistratie personen, de registratie van uitkeringsgerechtigden, het bijhouden van gegevens uit bouwaanvragen, het bijhouden van gegevens van mensen die een Wmo-voorziening hebben aangevraagd, en de uitvoering van de Jeugdwet en de gemeentelijke schulddienstverlening. De gemeente heeft als uitgangspunt én als wettelijke verplichting dat zij met deze gegevens behoorlijk en zorgvuldig omgaat in verband met de privacy van de betrokkenen.

Bescherming van persoonsgegevens is een grondrecht. Het verwerken van gegevens gebeurt op een faire, veilige en betrouwbare manier en inwoners worden op maat geholpen. De gemeente moet ook begrijpelijk uitleggen welke maatregelen het onrechtmatig gebruik van gegevens voorkomen. Een zorgvuldige omgang met de gegevens van inwoners vormt een essentiële bouwsteen voor het vertrouwen in de overheid. Bij privacybeleid gaat het niet alleen om naleving van de wet. Het leidt ook tot efficiënter werken, omdat het deel uitmaakt van het kwaliteitsbeleid. Met het gemeentelijk privacybeleid zorgen we voor een goed gedocumenteerd stelsel van interne afspraken waarmee we persoonlijke en gemeentelijke belangen kunnen waarborgen.

In deze beleidsnota is verhoudingsgewijs veel aandacht besteed aan het sociale domein. Wanneer inwoners een beroep doen op ondersteuning en/of hulp door de gemeente, worden immers vaker dan voorheen hun persoonsgegevens buiten de gemeentelijke organisatie verwerkt. Dit beleidsdocument stelt de algemene kaders vast waarbinnen de gemeente de privacy van inwoners regelt. Ook bepaalt het de richting voor het nader vast te stellen thematisch beleid.

Uit berichten in de media en uit gegevens van het College bescherming persoonsgegevens (CBP) blijkt dat het niet adequaat verwerken van persoonsgegevens een bron van ergernis is bij inwoners, zeker als de verwerking in strijd is met de wet. Het kan zelfs leiden tot onacceptabele situaties, waarbij bijvoorbeeld iemands identiteit wordt 'gestolen' en misbruikt. De juiste toepassing van wettelijke regels is van groot belang. Dit beleid vormt een nadere uitwerking van de wettelijke regelgeving en is daarnaast een praktische handleiding voor de ambtelijke organisatie.

Het CBP streeft voortdurend naar een behoorlijke en zorgvuldige verwerking van persoonsgegevens. Natuurlijk moet de gemeente over een goed stelsel van processen, werkafspraken en contracten beschikken om de privacy te kunnen waarborgen. Dat is in het belang van de inwoner én van de gemeente. Maar processen en protocollen worden uitgevoerd door mensen. Daarom streeft de gemeente naar een actief privacybeleid dat vooral gericht is op bewustwording, een open en kritische cultuur en kennisoverdracht.

2. Ambitie

De gemeente levert vele verschillende soorten diensten en biedt ondersteuning aan haar inwoners. Het is onontkoombaar dat daarbij informatie over personen wordt verwerkt. De verwerking van persoonsgegevens is inherent aan de gemeentelijke taakuitoefening. Voor een goede en zorgvuldige dienstverlening moet de gemeente gegevens van inwoners bewerken en soms met andere instanties delen. Informatieverwerking gaat gepaard met de verantwoordelijkheid om effectieve privacybescherming te bieden.

De gemeente vindt dat inwoners moeten kunnen vertrouwen op een veilige verwerking van persoonsgegevens. Niet alleen vanwege de wettelijke verplichting en de beheersing van bestuurlijke risico's, maar vooral ook omdat in deze informatiesamenleving de digitale leefbaarheid van inwoners bij de gemeente hoog in het vaandel staat. Vertrouwen in de publieke dienstverlening is van groot belang.

Onze gemeente vindt privacy een maatschappelijk vraagstuk en zoekt daarom actief naar manieren om inwoners te betrekken bij dit onderwerp en de bijbehorende dilemma's. Goede privacy-services, communicatie, transparantie en dialoog met inwoners vormen het fundament van ons privacybeleid.

3. Reikwijdte

Het gemeentelijk privacy beleid is van toepassing op alle taken en processen waar de gemeente verantwoordelijk voor is. Het privacy beleid is gebaseerd op de volgende uitgangspunten:

- Gegevens van burgers worden binnen de kaders van de geldende wet- en regelgeving verwerkt. Dit gebeurt uitsluitend als dit nodig is voor goede gemeentelijke taakuitoefening;
- Voor het bereiken van het doel waarvoor we de persoonsgegevens verwerken, beperken we de inbreuk op de persoonlijke levenssfeer van de betrokken inwoner zoveel mogelijk (subsidiariteit);
- De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn, in verhouding tot het te dienen doel (proportionaliteit);
- Gegevens worden gebruikt voor duidelijk omschreven doelen. Voor andere doelen worden ze enkel gebruikt of gedeeld wanneer de wet dat toestaat;
- De gemeente communiceert transparant hoe we over privacy denken en hoe we privacy borgen. Inwoners worden in algemene zin proactief geïnformeerd over wat met zijn of haar informatie gebeurt en waarom. In het thematisch beleid werken we nader uit of en in hoeverre we in individuele gevallen nadere informatie aan inwoners verstrekken;
- Bij de verwerking van persoonsgegevens ziet de gemeente erop toe dat de werkwijzen worden vastgelegd en professioneel worden uitgevoerd conform functionele en praktische protocollen of procesbeschrijvingen;
- Gegevens zijn steeds voldoende actueel en ze zijn een nauwkeurige weergave van de feitelijke situatie;
- De afhandeling van klachten en verzoeken van inwoners en bedrijven over hun privacy gebeurt op een toegankelijke, laagdrempelige wijze;
- Bij samenwerking met externe partners (specifiek binnen het sociale domein), waarbij sprake is van verwerking van persoonsgegevens, spreken we af aan welke de eisen de gegevensuitwisselingssystemen moeten voldoen. Door middel van in-control-statements wordt jaarlijks verantwoording afgelegd aan het college. Veel voorkomende processen die voor het werk belangrijk zijn, worden in specifieke procedures beschreven. Daarbij geven we aan hoe we met privacygevoelige informatie omgaan. Die specifieke procedures moeten voldoen aan de uitgangspunten van dit gemeentebrede beleid en natuurlijk aan het wettelijk kader. Dergelijke specifieke procedures (werkprocessen) worden ter vaststelling voorgelegd aan het college;
- De gemeente is altijd (eind)verantwoordelijk voor de gegevensverwerking en de privacy daarvan. Dit geldt ook als we gegevens ter beschikking stellen aan derden of delen in samenwerkingsverbanden.

4. Governance

De manier waarop we het privacybeleid binnen de gemeente verankeren, vormt het fundament van de privacyborging. Volgens de Wet bescherming persoonsgegevens is het college van burgemeester en wethouders verantwoordelijk voor de juiste uitvoering ervan. Deze paragraaf geeft aan hoe we de taken, verantwoordelijkheden en borging van het privacybeleid binnen de gemeente organiseren. Hoewel de gemeente nu al de privacyrechten van haar inwoners borgt, vraagt de implementatie van dit beleidsplan tijd en inzet van medewerkers. In 2015 wil de gemeente de inhoud, zoals in deze paragraaf omschreven, inrichten. In 2016 gaan we de werking verder optimaliseren.

4.1 Relatie met de raad

Het college is verantwoordelijk voor de juiste naleving van de Wet bescherming persoonsgegevens. Deze wet reikt daarvoor de basisset van privacy management controls aan. Het college informeert de raad binnen de jaarlijkse planning en control cyclus over de risico's en over de getroffen beheersmaatregelen binnen de processen waar de gemeente voor verantwoordelijk is. Om te zorgen dat inwoners de overheid vertrouwen, wil de gemeente op transparante wijze informatie verstrekken en verantwoording afleggen over het privacybeleid en daarmee over belangrijke rechten van onze inwoners.

4.2 Vastleggen van verantwoordelijkheden binnen de gemeente

4.2.1 Vaststelling van privacybeleid

Het college stelt het gemeentelijk privacybeleid vast. Het neemt daarbij de aanbevelingen van de privacyfunctionaris (zie onder 4.2.3) in acht en het bevordert de beschikbaarheid van voldoende middelen om privacy bescherming passend te waarborgen.

4.2.2 Uitvoering van privacybeleid

Het college wijst uit zijn midden een portefeuillehouder privacy aan. Deze is bestuurlijk verantwoordelijk voor de uitvoering van het gemeentelijk privacybeleid en voor de controle op de naleving van afspraken. De feitelijke uitvoering wordt opgedragen aan een ambtelijk medewerker (privacyfunctionaris, zie onder 4.2.3). Deze draagt daar samen met een team van professionals (de privacy- en informatiebeveiligingswerkgroep, zie onder 4.3.6) zorg voor.

4.2.3 Toezicht

Voor onafhankelijk toezicht op de uitvoering van het privacy beleid wijst het college een functionaris voor de gegevensbescherming (ook wel privacy functionaris genoemd) aan conform artikel 62-64 van de Wet bescherming persoonsgegevens. De privacyfunctionaris fungeert tevens als privacy ombudsman en is in voorkomende gevallen de liaison met de landelijke ombudsman. Zijn positie en taakuitoefening worden nader geregeld in een statuut dat het college vaststelt.

4.2.4 Beheer van het beleid

De privacyfunctionaris is de beheerder van het gemeentelijk privacybeleid, in samenspraak met de privacy- en informatiebeveiligingswerkgroep. De privacyfunctionaris brengt verslag uit aan het college over de voortgang en kwaliteit van de uitvoering van het privacybeleid en doet aanbevelingen voor verdere optimalisering.

4.2.5 Verantwoordelijkheid voor het ontwikkelen van thematisch beleid

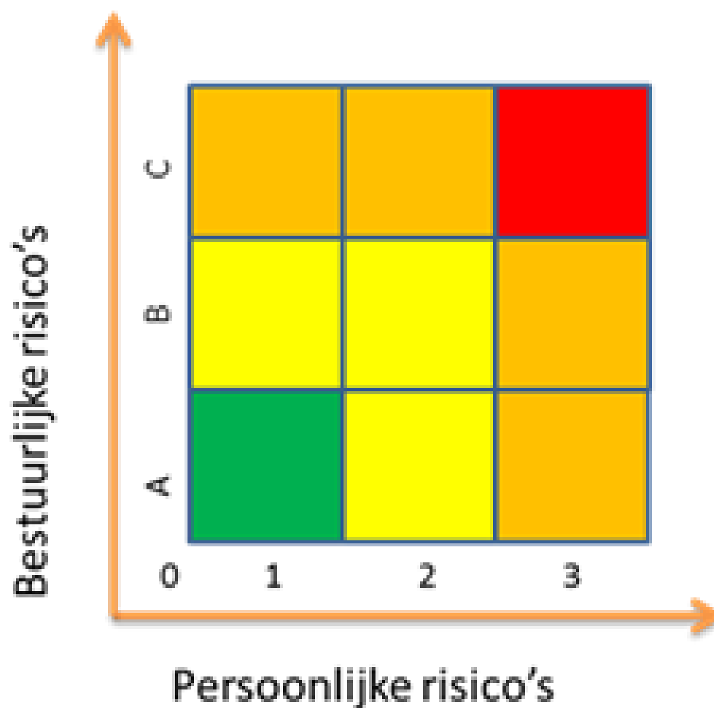
De portefeuillehouder privacy is bestuurlijk verantwoordelijk voor het ontwikkelen van het thematisch beleid. Namens hem ziet de privacyfunctionaris toe op de feitelijke ontwikkeling en uitvoering van themagericht privacybeleid (themabeleid), zoals de Basisregistratie Personen, Participatie en Jeugd. Een leidinggevende is hiervan proceseigenaar. Die krijgt ondersteuning van de privacy- en informatiebeveiligingswerkgroep.

4.2.6 Ontwikkeling van themabeleid en praktische privac waarborgen

De proceseigenaar is verantwoordelijk voor de ontwikkeling en uitvoering van themabeleid binnen de door het college gestelde kaders. Onder ontwikkeling en uitvoering van themagericht privacybeleid verstaan we met name: aantoonbare concretisering van beleid in praktische privacywaarborgen (documenteren), zodat ook op operationeel niveau structureel sprake is van behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet. Hierbij maken we bij voorkeur gebruik van bestaande oplossingen, voor zover uit toetsing blijkt dat deze zijn in te passen.

4.2.7 Risico gedreven aanpak

De gemeentelijke uitvoering van het privacy beleid is evenwichtig. Oplossingen zijn gebaseerd op privacy impact assessments (PIA's). De effecten, zowel kansen als bedreigingen voor personen en de gemeente, zijn in kaart gebracht en zijn afgewogen op basis van de inhoud. De risico's worden door praktische, organisatorische en technische maatregelen beheerst. Een risicoanalyse (zie afbeelding) brengt de mate van persoonlijk en bestuurlijk risico in kaart. Deze vormt het vertrekpunt voor het maken van beleidskeuzes.



4.2.8 Interne verantwoording
Proceseigenaren rapporteren minimaal een keer per jaar aan de portefeuillehouder over de resultaten die zij hebben bereikt bij realisatie en beheer van passende privacymaatregelen. Zij melden hem onverwijld privacy-incidenten conform een vast te stellen incidentenprocedure. Wanneer proceseigenaren verantwoordelijkheden hebben overgedragen of uitbesteed, zorgen zij voor een gelijkwaardige vorm van verantwoording. Afspraken hierover leggen we schriftelijk vast.

4.2.9 Verantwoordelijkheid van audit
Namens de portefeuillehouder privacy ziet de privacyfunctionaris toe op de totstandkoming van een privacy-auditplan op basis van de uitgevoerde PIA's en de ijkpunten (key controls) van de gekozen beheersmaatregelen volgens het themabeleid en de nadere concretisering.

4.3 Privacy Control Systeem
Met een reeks maatregelen wil de gemeente waarborgen dat we continu werken aan het optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Juist omdat privacy voor een belangrijk deel mensenwerk is, moet op alle niveaus binnen de gemeente ruime aandacht zijn voor het cyclisch denken. Door privacy vast op de diverse agenda's te plaatsen, ontstaat een continu proces van veranderen en verbeteren. Door vanuit verschillende niveaus en rollen binnen de gemeente naar de kwaliteit van de uitvoering van privacy te kijken, ontstaat een evenwichtig systeem van 'checks and balances'. Hieronder beschrijven we de belangrijkste elementen van deze borging.

4.3.1 Planning en control proces
Privacy vormt een onderdeel van het planning en control proces van de gemeente. Het college informeert de raad binnen de jaarlijkse planning en control cyclus over de risico's en beheersmaatregelen met betrekking tot het privacybeleid.

4.3.2 Onderdeel plannen
Privacy is een vast onderdeel van alle (deel)plannen van de gemeente. Hierdoor ontstaat ruimte voor beleidsmatige verbeteringen.

4.3.3 In control statement
De gemeente gaat werken met in control statement. In deze verklaring leggen proceseigenaren jaarlijks verantwoording af. Daarbij vermelden ze of de uitvoering van processen rondom privacy volgens het beleid verloopt. Ze geven ook aan waar afwijkingen zijn en welke beheersmaatregelen worden getroffen.

4.3.4 Auditplan

Op basis van risicoanalyse wordt een privacy-auditplan opgesteld onder bestuurlijke verantwoordelijkheid van de portefeuillehouder privacy en de ambtelijke verantwoordelijkheid van de privacyfunctionaris.

4.3.5 Werkoverleg
Leidinggevenden en medewerkers maken privacy tot een onderdeel van hun werkoverleg. Hiermee werken we actief aan een open cultuur, aan het optimaliseren van kennis en een transparante procesuitvoering. Bevindingen of vragen kan iedereen voorleggen aan de privacy- en informatiebeveiligingswerkgroep.

4.3.6 Privacy- en informatiebeveiligingswerkgroep
De gemeente heeft een privacy- en informatiebeveiligingswerkgroep waarin enkele kernfuncties zijn vertegenwoordigd. De privacyfunctionaris maakt hiervan deel uit. De privacy- en informatiebeveiligingswerkgroep treedt op als adviseur voor het college, is een vraagbaak voor de medewerkers en leidinggevenden, en vormt de kern van het auditteam privacy.

4.3.7 Toezicht door de privacyfunctionaris
De privacyfunctionaris toetst of de aanwezigheid en werking van het gemeentelijk privacybeleid afdoende is ingericht. Hij heeft vrij toegang tot systemen en processen van de gemeente. Hij rapporteert rechtstreeks aan het college van burgemeester en wethouders. De privacyfunctionaris treedt ook op als ombudsman wanneer inwoners klachten hebben over de service van de gemeente bij de uitoefening van de privacyrechten en het privacybeleid.

4.4 Bemensing

4.4.1 Privacyfunctionaris
Het aanstellen van de een privacy functionaris is een belangrijke stap in het waarmaken van de maatschappelijke privacy-ambities. Bij de Europese privacywetgeving, te verwachten in 2016, wordt de aanstelling van zo'n functionaris waarschijnlijk verplicht. De gemeente stelt een privacyfunctionaris aan om het eigen toezicht te organiseren. Deze medewerker heeft een belangrijke coördinerende rol en adviseert over oplossingen met betrekking tot privacy. Belangrijk is ook dat hij aan de voorkant meekijkt bij de inrichting van processen. De privacyfunctionaris maakt deel uit van de gemeentelijke privacy- en informatiebeveiligingswerkgroep.

4.4.2 Gemeentelijke privacy- en informatiebeveiligingswerkgroe p
Binnen de gemeente wordt een privacy- en informatiebeveiligingswerkgroep gevormd. Die is de vraagbaak voor privacy vraagstukken, adviseert over beleid en uitvoering, draagt bij aan kennisverspreiding en cultuur, en heeft een rol binnen het interne audit programma. De privacy- en informatiebeveiligingswerkgroep wordt gerealiseerd door de bestaande (informatie)-beveiligingswerkgroep (die het merendeel van de gewenste rollen al bevat) uit te breiden met een jurist en de privacyfunctionaris. De werkgroep kan eventueel op afroep worden uitgebreid met communicatie en hoofd bedrijfsvoering. De privacyrollen zijn evenals de informatiebeveiligingsrollen onderdeel van het regulier werk.

4.5 Services richting inwoners

4.5.1 Transparantie
Rechten van de burger zijn binnen de gemeente op transparante wijze ingericht. Het recht op inzage, informatie, correctie en verwijdering van gegevens is vertaald in heldere, laagdrempelige procedures en wordt helder gecommuniceerd richting inwoners.

4.5.2 Meldingen en klachten
Meldingen en klachten over privacy komen bij de gemeente binnen via de bestaande kanalen. De proceseigenaar geeft de melding of klacht door aan de privacy- en informatiebeveiligingswerkgroep, waar deze wordt geregistreerd. De desbetreffende proceseigenaar is verantwoordelijk voor de afwikkeling en het treffen van eventuele verbetermaatregelen. Indien de inwoner hierover niet tevreden is, kan hij een klacht indienen bij de privacyfunctionaris.

5. Juridisch kader

De Wet bescherming persoonsgegevens (Wbp) regelt het algemene kader voor de omgang met privacy. Deze is te beschouwen als parapluwetgeving die van toepassing is op bijna alle sectoren, instellingen en bedrijven in Nederland. Voor het verwerken van persoonsgegevens voor privégebruik geldt de Wbp niet. De Wbp vereist dat voor elke verwerking van persoonsgegevens een beroep kan worden gedaan op één van de grondslagen die in artikel 8 van de Wbp worden genoemd. Na vaststelling van die grondslag is het mogelijk om gestructureerd te bepalen welke verwerking, van welke persoonsgegevens,

voor welke doeleinden rechtmatig en noodzakelijk is. Daarnaast zijn in tal van bijzondere wetten regels over privacy opgenomen. Bijlage B bevat een opsomming van de relevante regelgeving.

6. Bewustwording, communicatie en evaluatie

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, ambtenaren en hulpverleners moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van het belang van het waarborgen van de rechten van de inwoners. De samenleving maakt op dit moment een belangrijke kanteling door. Er wordt een groot beroep gedaan op saamhorigheid en zelfredzaamheid, met als doel: de eigen kracht van inwoners versterken. Mensen moeten ook minder afhankelijk worden van door de gemeente gefinancierde zorg en ondersteuning. De rijksoverheid wil dat burgers zelfstandig hun leven kunnen leiden, hun eigen problemen kunnen oplossen en een bijdrage leveren aan de samenleving. De burger moet meer regie voeren over zijn leven, maar ook over de uitvoering van de zorg. Dit geldt ook voor het betrekken van burgers bij privacyvraagstukken en het gebruik van persoonsgegevens. Soms zullen professionals en ambtenaren dit lastig vinden, maar uiteindelijk is het maatschappelijk gewenste effect hiermee het beste gediend. In een voor de burger onveilige en complexe situatie biedt de wet bij uitzondering mogelijkheden om anders om te gaan met bijvoorbeeld toestemming voor de uitwisseling van informatie. Dit is dan in het belang van de burger zelf.

Het is belangrijk dat personen die daadwerkelijk met persoonsgegevens werken, weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig met deze gegevens moeten omgaan. Professionals in het veld en binnen de gemeente moeten zich daarom bewust zijn van de regels en gedragsnormen rondom privacy. De gemeente ondersteunt dit door onder meer privacyprotocollen en afwegingskaders te ontwikkelen. Richting inwoners is communicatie over de privacy van belang. Inwoners hebben het recht te weten wat er met hun gegevens gebeurt.

De professionals moeten zich bewust zijn van het belang van privacy. Zij moeten persoonsgegevens op een zorgvuldige manier verwerken, zoals omschreven in het privacybeleid en de bijbehorende regelingen. Er worden trainingen georganiseerd over hoe zij vanuit hun functie/rol met privacyvraagstukken moeten omgaan. De gemeente streeft naar een cultuur waarbij professionals elkaar in alle openheid aanspreken op het eigen gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden om een optimaal privacybeleid te realiseren.

Dit alles moet binnen het privacybeleid worden verankerd. Het beleid wordt uiterlijk op 31 december 2016 geëvalueerd door middel van een Privacy Impact Assessment.

7. Uitgangspunten privacybeleid

De vorige paragrafen vormen een generiek beleidskader voor het gemeentelijk privacy beleid. Door de decentralisaties per 1 januari 2015, neemt de verwerking van (bijzondere) persoonsgegevens alsmaar toe. Daarom zoomen we hieronder kort in op de gegevensverwerking in het sociale domein.

De uitvoering van de gedecentraliseerde taken brengt met zich mee dat de gemeente en diverse instellingen en instanties gegevens moeten uitwisselen. In de wetten en daarop gebaseerde besluiten is - soms vrij nauwkeurig, soms meer in algemene termen - beschreven welke gegevens nodig zijn voor de taakuitoefening en welke instanties/instellingen bevoegd zijn om die te verstrekken (zie bijlage B). Bij het uitoefenen van die bevoegdheid moeten ze wel bepaalde principes in acht nemen: behalve doelbinding (die in de meeste gevallen dus rechtstreeks uit de wet voortvloeit) gaat het om de principes van subsidiariteit en proportionaliteit. Dit zijn ook de leidende principes van de Wet bescherming persoonsgegevens. Bovendien gelden er strengere eisen wanneer sprake is van bijzondere gegevens (met name gezondheidsgegevens en strafrechtelijke gegevens). Bij het verwerken van gegevens over de gezondheid van personen is in veel gevallen de Wet geneeskundige behandelingsovereenkomst leidend. Met het oog op de uitwisseling van bijzondere gegevens is het wenselijk om duidelijk te zijn over het beleid dat de gemeente hanteert voor de uitvoering in de praktijk. Hiervoor zijn de volgende uitgangspunten geformuleerd:

- Hulpverleningsperspectief in veel gevallen leidend;
- Gegevensverwerking op basis van 'need to know';
- Gegevensverwerking op basis van 'toestemming, tenzij';
- Zorg voor betrokkenheid van cliënt.

Hieronder volgt een nadere uitwerking van deze uitgangspunten.

7.1 Hulpverleningsperspectief in veel gevallen leidend

De gemeentelijke overheid is verantwoordelijk voor het toekennen van voorzieningen die voor een belangrijk deel betrekking hebben op hulpverlening, zoals zorg en ondersteuning. Soms met een gedwongen karakter, maar ook dan is sprake van hulpverlening. Een belangrijk aspect is dat er een vertrouwensrelatie ontstaat. Het in de hulpverlener gestelde vertrouwen is essentieel om taken goed te vervullen.

7.2 Gegevensverwerking op basis van 'need to know'

Dit uitgangspunt heeft enerzijds te maken met het vereiste van doelbinding: alleen die gegevens die noodzakelijk zijn vanuit een bepaald doel worden verwerkt. 'Need to know' is dus geen 'nice to know'. Bij dit uitgangspunt speelt ook de vraag in hoeverre bij verwerking wordt voldaan aan de uitgangspunten van proportionaliteit (niet meer privacy-inbreuk dan nodig) en subsidiariteit (ander middel dat minder inbreuk op privacy maakt om het gestelde doel te realiseren, heeft de voorkeur). Dit speelt vooral bij de verwerking van gegevens in het kader van signalering en bij de vraag hoe lang gegevens moeten worden bewaard. Het is belangrijk dat al vanaf het begin (toegang) prioriteiten worden gesteld en de privacy-inbreuk zo beperkt mogelijk blijft. Dat gebeurt door een goede vraaganalyse of vraagverheldering.

7.3 Gegevensverwerking op basis van 'toestemming, tenzij'

Gegevensverwerking vindt eerst en vooral plaats met toestemming van de betrokkene. In geval van hulpverlening betekent toestemming voor de behandeling ook toestemming voor gegevensverwerking. Is er eenmaal sprake van toestemming voor de behandeling (tevens: begeleiding en verzorging), dan hoeft niet ook nog eens afzonderlijke toestemming te worden gevraagd voor het delen van gegevens tussen zorgverleners die rechtstreeks bij de behandeling zijn betrokken. In bijlage B is dit verder uitgewerkt onder het kopje Jeugdwet.

Soortgelijke bepalingen zijn ook opgenomen in de Wet op de geneeskundige behandelingsovereenkomst (Wgbo). Wie rechtstreeks betrokken zijn bij de behandeling, is op te maken uit het ondersteuningsplan dat de betrokkene ondertekent. Nadrukkelijk wordt aangetekend dat het verlenen van toestemming niet de enige grond is voor de verwerking van persoonsgegevens. In artikel 8 van de Wbp staat een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen. Er moet altijd sprake zijn van transparantie. Een burger moet immers gebruik kunnen maken van zijn recht op verzet.

7.4 Zorg voor betrokkenheid van cliënt

Hoe meer de cliënt het gevoel heeft dat hij echt wordt betrokken, hoe minder noodzakelijk het is om hem voor diverse handelingen vooraf toestemming te vragen. Dit heeft veel te maken met het begrip transparantie, een begrip waarop vooral de in de Wgbo uitgewerkte informatieplicht is gebaseerd. Uitgangspunt bij overleg moet zijn dat we niet óver de cliënt, maar mét de cliënt praten.

8. Convenanten en overeenkomsten

Met het oog op de omgang met privacy door alle partijen waar de gemeente mee samenwerkt en waarbij persoonsgegevens worden verwerkt, worden convenanten, bewerkersovereenkomsten en protocollen afgesloten. De gemeente moet de eisen rondom gegevensverwerking borgen in contracten. Hier moet tevens de grondslag worden gelegd voor het laten uitvoeren van een privacy-audit. Ook wordt hierbij verwezen naar de bijbehorende privacymatrix (zie bijlage C). Hoe we afspraken maken met ketenpartners is sterk afhankelijk van de positie in de informatieketen en de aard van de samenwerking. Hierin wordt in ieder geval aangegeven:

- De betrokken organisaties, verantwoordelijken en relevante doelstellingen;
- De verwerking van bijzondere persoonsgegevens;
- De wijze waarop betrokken inwoners worden geïnformeerd over het gebruik van hun persoonsgegevens;
- De belangrijkste verwerkingen van persoonsgegevens die binnen de samenwerking plaatsvinden, de melding daarvan bij het College bescherming persoonsgegevens en de eenduidige protocollering van de privacyregels die bij de verwerking in acht genomen moeten worden;
- De wijze waarop we bij betrokken inwoners toestemming verkrijgen voor gegevensverwerking;

- Een beschrijving van de gevallen waarin zonder toestemming van de betrokkene gegevens worden verwerkt;
- Een beschrijving van een procedure in verband met escalatie bij spoed- en/of noodgevallen;
- De wijze waarop betrokkenen gebruik kunnen maken van hun rechten op grond van de Wet bescherming persoonsgegevens. De wijze waarop organisaties invulling geven aan informatiebeveiliging en geheimhoudingsplicht.

vastgesteld door het College van Burgemeester en Wethoudersvan de gemeente Echt-Susteren op 9 juni 2015

Bijlage 1: Functionaris voor de gegevensbescherming (privacyfunctionaris)

In deze bijlage wordt uitgelegd wat de rol van privacyfunctionaris inhoudt. Voor privacyfunctionaris wordt hierna de wettelijke term gehanteerd: functionaris voor de gegevensbescherming (FG).

Privacytoezicht algemeen

Om de rol van FG goed te begrijpen, moet hier eerst het toezichtsysteem van de Wet bescherming persoonsgegevens (Wbp) worden uitgelegd, want de Wbp regelt toezicht op verschillende manieren.

Waar meestal als eerste aan wordt gedacht, is het toezicht door de landelijke toezichthouder, het College bescherming persoonsgegevens (CBP). Maar de Wbp kent ook aan het college van burgemeester en wethouders een toezichthoudende rol toe, als regievoerder en de controleur op nakoming van afspraken. Daarnaast zijn ook burgers in zekere zin toezichthouder, omdat de Wbp hen het recht toekent om bij de gemeente de verwerking van hun eigen gegevens te controleren. Ze hebben het recht op schadevergoeding wanneer het gemeentelijk privacybeleid tekort schiet en ze mogen bij het CBP een handhavingsverzoek indienen.

Daarmee is de Wbp een systeem van ‘checks and balances’. Dit systeem werkt echter niet goed, zolang er geen FG is aangewezen. Dit komt onder meer doordat privacy een complex vraagstuk is, dat ook met misverstanden is omgeven. Het CBP staat op een te grote afstand om op reguliere wijze privacybeleidsvoering van een gemeente te kunnen controleren.
De aanwijzing van een FG- eveneens een toezichthouder die in de Wbp wordt genoemd - is daarom een logische zaak. Zéker omdat de nieuwe gemeentelijke taken in het sociaal domein extra privacy risico's met zich meebrengen.

Wat is een FG?

De FG laat zich het beste vergelijken met een accountant. Het grote verschil is echter dat de FG advies en toezicht juist niet mag scheiden, maar moet combineren.

Een FG denkt mee over privacybestendige oplossingen (preventief toezicht), maar toetst ook achteraf of oplossingen daadwerkelijk binnen de kaders van de wet zijn vormgegeven (privacy audits). Zijn aanbevelingen zijn bestemd voor het college van burgemeester en wethouders. Dat neemt niet weg dat de FG in de praktijk vooral samenwerkt met afdelingen en tweede lijn-professionals, zoals informatiemanagers, informatiebeveiligers, juristen en ICT-ers.

Functieprofiel FG

De FG is een multidisciplinaire senior. De wet vereist dat hij voldoende betrouwbaar is en stevig genoeg in zijn schoenen staat om onafhankelijk te kunnen adviseren. Hij moet praktijkdeskundig zijn (kennis van organisaties, processen, ICT en informatiebeveiliging) en een expert op het gebied van privacywetgeving. Nog afgezien van zijn interne betrokkenheid, speelt hij ook extern een belangrijke rol. Hij geeft het gemeentelijk privacybeleid een gezicht en heeft een bufferfunctie in de relaties met het College bescherming persoonsgegevens. Een FG moet daarom een goed gevoel hebben voor interne en externe verhoudingen en moet beschikken over vaardigheden op het gebied van communicatie, public relations en regulatory affairs.

Positie FG

De positie van de FG wordt beschreven in paragraaf 2 van hoofdstuk 9 Wbp over derde lijn-toezicht. Paragraaf 1 van dit hoofdstuk regelt de positie van het CBP. De wet bevat geen bepalingen over een hiërarchische relatie.
De FGis dus geen verlengstuk van het CBP. Wél is het zo dat de FG bij twijfel het recht heeft om het CBP te consulteren. Mits dat goed is aangepakt, kan dat helpen om bij het CBP begrip te kweken voor de gemeentelijke aanpak. Het CBP hecht veel waarde aan de aanwijzing van FG's. Organisaties met een FG genieten bij de landelijk toezichthouder extra vertrouwen.

Vanwege zijn wettelijke rol en deskundigheid, is het oordeel van de FG juridisch zwaarwegend. In de praktijk wordt dat echter niet altijd begrepen. Ook komt het voor dat op een FG druk wordt uitgeoefend om zijn zienswijze te herzien. Het is belangrijk om dit soort dingen van te voren door te spreken. Een FG moet veilig kunnen adviseren en moet daarvoor goed de ruimte krijgen. De wet geeft aan dat hij niet uit zijn functie kan worden gezet. Om over dit soort zaken duidelijk te zijn, verdient het sterk de aanbeveling om zijn positie te regelen in een statuut.

Door een FG aan te wijzen, functioneert het CBP meer op de achtergrond. Het CBP treedt weer op de voorgrond wanneer het gemeentelijk toezicht niet goed blijkt te functioneren.

Aanwijzing FG

De aanwijzing van een FG wordt onder de Wbp aanbevolen en wordt onder de nieuwe EU-privacyverordening (invoering naar verwachting in 2016) hoogstwaarschijnlijk verplicht. Hij kan in dienst zijn of worden genomen, worden ingehuurd of worden betrokken via een organisatie waarbij een gemeente is aangesloten.

Het college van burgemeester en wethouders moet over de aanwijzing van een FG besluiten en dat vervolgens melden bij het CBP[1]• Dat neemt zijn gegevens over in het openbare FG-register[2]. Het CBP beoordeelt niet de geschiktheid van de FG. De aanwijzing van een gekwalificeerde privacyfunctionaris blijft dus de eigen verantwoordelijkheid van het college. De geschiktheid van een FG kan blijken uit zijn CV (studie, werkervaring, publicaties, bij voorkeur een certificaat van de IAPP, de Internationale Associatie van Privacy Professionals, etc.).

Het salarisniveau van een FG ligt in Nederland gemiddeld op schaal 11-12, wat lager is dan in andere EU-landen (schaal 13-14) [3]. Het salaris hangt ook samen met de mate waarin de FG een coördinerende/leidinggevende rol heeft.

Een FG heeft kantoorfaciliteiten, tooling en overige middelen nodig voor professionele invulling van zijn taken. Hiervoor zijn ook lean & mean-oplossingen denkbaar. Het scheelt wanneer de FG kan rekenen op een werkgroep van tweede lijn-professionals.

[1] 1https://cbpweb.nl/sites/default/files/atoms/files/fg aanmeldingsformulier.pdf
[2] https://cbpweb.nl/nl/zelf-doen/functionaris-gegevensbescherming/register-functionarisgegevensbescherming-e-tm-h
[3] Onderzoek NGFG,gepubliceerd in *Privacy & Compliance* 04-05/2013

Bijlage 2: Toelichting wettelijke kaders

a) Jeugdwet

Grondslag: taken waarvoor verwerking van persoonsgegevens is toegestaan

Voor de volgende taken is in de Jeugdwet een grondslag opgenomen voor verwerking van persoonsgegevens:

- De toeleidingstaak;
- Jeugdhulpplicht;
- Het doen van een verzoek tot onderzoek aan de Raad voor de Kinderbescherming;
- Het (laten) uitvoeren van kinderbeschermingsmaatregelen en jeugdreclassering;
- De financiering van jeugdhulp, kinderbeschermingsmaatregelen en jeugdreclassering.

Toestemming voor jeugdhulpverlening en dossiervoering Jeugdhulp wordt, met inachtneming van een in de wet vastgelegde informatieplicht, verleend met toestemming van betrokkene. Tenzij het hulp betreft in het gedwongen kader (kinderbeschermingsmaatregelen of jeugdreclassering die door de rechter zijn opgelegd). Er zijn twee uitzonderingen hierop:

- Voor kinderen met een leeftijd tussen 12 en 16 jaar: toestemming van ouders met gezag of voogd is vereist. Tenzij de betrokkene bij weigering van de toestemming de hulp weloverwogen blijft wensen of indien die hulp kennelijk nodig is om ernstig nadeel voor de betrokkene te voorkomen.
- Voor personen van zestien jaar en ouder die niet in staat kunnen worden geacht tot een redelijke waardering van hun belangen ter zake: dan de jeugdhulpverlener en de curator of mentor uit te gaan van een weigering als dit blijkt uit de kennelijke opvatting van betrokkene op basis van eerdere uitingen toen betrokkene nog wel in staat was tot een redelijke waardering van belangen. De jeugdhulpverlener kan hiervan echter afwijken als hij daartoe gegronde redenen aanwezig acht.

De jeugdhulpverlener heeft de plicht om voor de hulp aan de betrokkene een dossier in te richten en bij te houden. Hieraan moet hij desgevraagd een door de betrokkene afgegeven verklaring toevoegen. Er geldt een bewaartermijn van tenminste vijftien jaar. Verder moet het dossier (of delen daarvan) op verzoek van de betrokkene binnen drie maanden worden vernietigd, tenzij aannemelijk is dat bewaring van aanmerkelijk belang is voor een ander of een wettelijke regeling zich hiertegen verzet.
De jeugdhulpverlener moet zorgen dat hij niet zonder toestemming informatie over de betrokkene (of inzage in of afschrift van het dossier) aan anderen verstrekt. Onder deze anderen zijn niet begrepen:

- rechtstreeks bij de hulpverlening betrokkenen en degenen die de jeugdhulpverlener vervangen, voor zover dit noodzakelijk is voor de taakuitoefening;
- de curator of mentor van betrokkene; verstrekking gebeurt alleen wanneer daardoor de persoonlijke levenssfeer van de ander niet wordt geschaad.

De verstrekking kan ook opgelegd zijn bij of krachtens de wet. Dan gelden er geen beperkingen. Verder kan de jeugdhulpverlener altijd besluiten geen informatie verstrekken wanneer hij dit in strijd acht met goed hulpverlenerschap.

Alle hierboven genoemde verplichtingen gelden jegens ouders die het gezag over de betrokkene uitoefenen of diens voogd wanneer de betrokkene nog geen 12 jaar is. Datzelfde geldt in de gevallen dat de betrokkene ouder is dan 12, maar niet in staat wordt geacht tot het redelijk waarderen van zijn belangen. Tenzij de betrokkene meerderjarig is en er een mentor of curator is benoemd voor wie de verplichtingen gelden. Is er geen mentor of curator, dan is de volgorde: schriftelijk gemachtigde, echtgenoot/geregistreerde partner/levensgezel (tenzij deze dat niet wenst), ouder, kind, broer of zus (tenzij deze dat niet wenst).
De verplichtingen zijn niet *van* toepassing als deze niet verenigbaar zijn met de zorg *van* een goede hulpverlener. Ook geldt dat de vertegenwoordiger zijn taak goed moet vervullen en de betrokkene hier *zoveel* mogelijk bij betrekt. Mocht die zich verzetten, dan kan alleen zonder toestemming worden ingegrepen wanneer dat kennelijk nodig is om ernstig nadeel *voor* de betrokkene te voorkomen.

Gebruik Burgerservicenummer

De gecertificeerde instelling, de jeugdhulpaanbieder, de Raad voor de Kinderbescherming en het college (lees: de gemeente) moeten bij hun taakuitoefening gebruikmaken van het Burgerservicenummer van de betrokkene. Uitzondering daarop geldt bij de uitwisseling van gegevens in het kader van de jeugdreclassering voor het strafrecht en bij situaties waar afwijking van deze regel noodzakelijk is vanwege spoedeisende gevallen. De gemeente moet conform de wettelijke eisen zorgen voor de uitvoering van

reclassering en jeugdhulp. Daarom is geregeld dat de Minister van Justitie en Veiligheid in een strafrechtelijke beslissing het Burgerservicenummer van een jeugdige kan verstrekken. Hij doet dat aan een ambtenaar of aan een onder zijn verantwoordelijkheid werkzame functionaris (beiden moeten daarvoor door het college zijn aangewezen).

b) Wet maatschappelijke ondersteuning 2015

Bevoegdheid toezichthouders

Toezichthoudende ambtenaren mogen - voor zover dat noodzakelijk is in het kader van hun taak - inzage in dossiers vragen. Uiteraard zijn ze daarbij gebonden zijn aan dezelfde geheimhoudingsplicht die voor de aanbieder geldt. Uitzonderingen: bij wilsonbekwaamheid van de betrokkene of indien noodzakelijk ter bescherming van cliënten.

Grondslag: taken waarvoor verwerking van persoonsgegevens is toegestaan

Om te beoordelen of iemand in aanmerking komt voor een Wmo-voorziening, een Pgb of om het verhaalsrecht uit te oefenen, mogen de uit onderzoek verkregen persoonsgegevens (waaronder gezondheidsgegevens) worden verwerkt. Persoonsgegevens van de mantelzorger van de cliënt mogen worden verwerkt. Maar alleen voor zover ze nodig zijn om te bepalen welke hulp deze aan de cliënt kan bieden, en voor zover deze zijn verkregen van de cliënt of de mantelzorger, en als deze noodzakelijk zijn voor de uitvoering van de wet. Een soortgelijke bepaling is opgenomen met betrekking tot persoonsgegevens van andere personen in het sociaal netwerk van de cliënt. Indien uit een melding een redelijk vermoeden van huiselijk geweld kan worden afgeleid, mag Veilig Thuis (Advies- en Meldpunt Kindermishandeling / AMHK) persoonsgegevens registreren van personen die bij het huiselijk geweld zijn betrokken. De gemeente mag bepaalde persoonsgegevens verstrekken aan aanbieders van Wmo-voorzieningen, het CAK,de instantie die de eigen bijdrage int, de Sociale Verzekeringsbank en toezichthoudende ambtenaren.

Toestemmingsvereiste bij afstemming van hulp in het kader van uitvoering van andere wetten en bij het opvragen van persoonsgegevens bij de zorgverzekeraar

Ondubbelzinnige toestemming van betrokkene is vereist voor de verwerking van persoonsgegevens van betrokkene zelf dan wel van personen in zijn directe omgeving, met het oog op een goede afstemming van de hulp in het kader van aan de gemeente opgedragen taken in andere wetten (Jeugdwet, Participatiewet, Wet gemeentelijke schuldhulpverlening), ervan uitgaande dat dit noodzakelijk is voor uitvoering van de wet. Dat geldt ook voor persoonsgegevens van de betrokkene die bij een zorgverzekeraar worden opgevraagd.

Uitzondering op toestemmingsvereiste bij verstrekken gegevens aan Veilig Thuis (AMHK)

Derden die beroepshalve beschikken over inlichtingen die kindermishandeling kunnen beëindigen of nodig zijn om een redelijk vermoeden van kindermishandeling te onderzoeken, kunnen deze gevraagd en ongevraagd aan Veilig Thuis (Advies- en Meldpunt Kindermishandeling / AMHK) verstrekken zonder toestemming van degene die het betreft. Zo nodig met doorbreking van de pllcht tot geheimhouding op grond van de wet, hun ambt of beroep.

Identificatieplicht

De cliënt is verplicht om zich te identificeren bij de aanbieder van een maatwerkvoorziening.

Gebruik Burgerservicenummer

De gemeente, Veilig Thuis (AMHK), aanbieders, toezichthouders en andere uitvoerende instanties zijn bij verstrekkingen verplicht om gebruik te maken van het Burgerservicenummer van de betrokkene.

Informatieplicht bij meldingen Veilig Thuis (AMHK)

Bij meldingen bij Veilig Thuis (AMHK) door een ander dan de betrokkene, wordt de betrokkene zo spoedig mogelijk, maar in ieder geval binnen vier weken, hiervan op de hoogte gesteld. Uitstel is alleen mogelijk als dit noodzakelijk is om een situatie van huiselijk geweld te beëindigen of een redelijke vermoeden daarvan te onderzoeken.

Uitoefening privacy rechten bij Veilig Thuis (AMHK)

Geclausuleerd recht op inzage, afschrift en vernietiging van persoonsgegevens op verzoek van de betrokkene.

Gebruik persoonsgegevens voor onderzoek

Het recht om zonder voorafgaande toestemming van de betrokkene persoonsgegevens te verstrekken voor statistiek of wetenschappelijk onderzoek. Hierbij gelden strenge voorwaarden als uitwerking van de principes van subsidiariteit en proportionaliteit. Ook geldt de restrictie dat de betrokkene niet uitdrukkelijk bezwaar heeft gemaakt.

c) Participatiewet

De Wet werk en bijstand is per 1 januari 2015 overgegaan in de Participatiewet. Vanaf dat moment is deze wet toegankelijk voor een bredere doelgroep; voor iedereen die voorheen een beroep deed op de Wajang (Wet werk en arbeidsondersteuning jonggehandicapten) of de Wsw (Wet sociale werkvoorziening).

Gegevensverwerking en Suwinet-Inkijk

Gegevensverwerking in de Participatiewet is geregeld conform een gesloten verstrekking regime om zo de privacy van burgers binnen de sociale zekerheid zo goed mogelijk te waarborgen. Dat regime houdt in dat werk en inkomen gegevens uitsluitend worden hergebruikt als daar een wettelijke grondslag voor is of als de burger daar toestemming voor heeft gegeven. Bij het uitvoeren van de Participatiewet maakt werk en inkomen gebruik van de landelijk beschikbare applicatie Suwinet-Inkijk. Suwinet-Inkijk mag niet voor andere doeleinden gebruikt dan voor de uitvoering van de Participatiewet. Via deze Inkijk mogen gegevens in het kader van de Wet structuur en uitvoeringorganisatie werk en inkomen (Wet SUWI) en de Wbp tussen organisaties binnen
het SUWI-stelsel worden uitgewisseld. Maar gegevens van werkzoekenden mogen in beginsel alleen aan organisaties buiten SUWI worden verstrekt, als daar een uitdrukkelijke wettelijke grondslag of verplichting voor bestaat of als de cliënt daar toestemming voor heeft gegeven.

Grondslag voor verwerking gegevens werkzoekende, inlichtingenplicht

De uitvoering van de wettelijke taken op het gebied van werk en inkomen brengt met zich mee dat er veel privacygevoelige gegevens worden verwerkt. Zo wordt aan werkzoekenden gevraagd naar hun tijdsbesteding en dagritme, maar ook naar het gebruik van alcohol en verdovende middelen. Verder worden vragen gesteld over medische aangelegenheden, zoals het gebruik van geneesmiddelen, lichamelijke beperkingen en eventuele sociale of psychische problemen. Een werkzoekende is verplicht om mee te werken en de gevraagde gegevens te verstrekken. Een werkzoekende heeft echter ook recht op privacy. De gemeente moet daarom
altijd aan de cliënt duidelijk kunnen maken waarom het noodzakelijk is dat hij bepaalde gegevens aan de gemeente verstrekt. Een inbreuk op de persoonlijke levenssfeer mag alleen plaatsvinden als daar een wet aan ten grondslag ligt en de inbreuk noodzakelijk is in het kader van de uitvoering van die wet.

Grondslag voor verwerking gegevens van verwanten/huisgenoten

De gemeente heeft soms gegevens nodig van kinderen of inwonende ouders van de werkzoekende. Het gaat dan bijvoorbeeld om inkomensgegevens van meerderjarige kinderen in verband met de afdracht van kostgeld en de berekening van het gezinsinkomen of om inkomensgegevens van de ex-partner in verband met de afdracht van alimentatie. Gegevensvan verwanten van de werkzoekende moeten bijzondere aandacht krijgen. Ze worden door de betrokkenen doorgaans ervaren als een grote inbreuk op hun privacy. Het vragen van gegevensvan derden moeten we daarom tot een minimum beperken. Gegevensvan verwanten kunnen nodig zijn om bijvoorbeeld het gezinsinkomen te bepalen of om vast te stellen of de aanvrager recht heeft op een uitkering. Voor deze mensen moet het duidelijk zijn waarom ze hun gegevens moeten verstreken, in relatie tot de uitkering van de werkzoekende.

Inlichtingenverplichting instanties

In de Participatiewet zijn de instanties vermeld die verplicht zijn om aan de gemeente kosteloos opgaven en inlichtingen te verstrekken die noodzakelijk zijn voor de uitvoering van de wet. De niet vermelde instanties geldt moeten zelf afwegen of verstrekking van de gegevens aan de gemeente verenigbaar is met het doel waarvoor zij de gegevens hebben verkregen en gebruiken. In een aantal gevallen is het instanties (of personen) verboden om inlichtingen aan de gemeente te verstrekken. Het gaat dan om personen die uit hoofde van hun beroep of functie een geheimhoudingsplicht hebben, zoals medici en paramedici op grond van de Wet geneeskundige behandelingsovereenkomst (Wgbo), de Wet Beroeps-

beoefenaren individuele gezondheidszorg (BIG)of hun beroepscode. Denk bijvoorbeeld aan huisartsen, keuringsartsen en psychologen. Gegevensverstrekking aan de gemeente door personen of instanties met een geheimhoudingsplicht kan alleen na (vrijwillig gegeven) schriftelijke toestemming van de werkzoekende (machtiging). Verder is in de Participatiewet vastgelegd dat bij verstrekkingen door het college, het inlichtingenbureau en de in de wet genoemde instanties, indien daartoe bevoegd, gebruik moeten maken van het Burgerservicenummer.

Geheimhoudingsplicht, wettelijke grondslag of toestemming voor verstrekking

Voor iedereen die bij de uitvoering van de Participatiewet betrokken is, geldt een geheimhoudingsplicht. Wat hem wordt medegedeeld mag hij niet verder bekend maken dan voor de uitvoering van de wet noodzakelijk is, dan wel op grond van de wet is voorgeschreven of toestaan. Verstrekking aan niet bij wet of regeling benoemde instanties is alleen mogelijk met schriftelijke toestemming van de werkzoekende. Wel kunnen desgevraagd gegevens aan derden worden verstrekt voor wetenschappelijke onderzoek of statistiek voor zover de persoonlijke levenssfeer van de betrokkenen daardoor niet onevenredig wordt geschaad. Indien er een wettelijke grondslag is voor verstrekking aan de gemeente, moet de verstrekker nagaan of degene aan wie hij de gegevens verstrekt redelijkerwijs bevoegd is te achten om die gegevens te verkrijgen.

Geen algemene machtiging en geen dwang

Algemeen geformuleerde machtigingen, waarmee de werkzoekende toestemming geeft aan derden om inlichtingen te verschaffen aan de gemeente, zijn niet toegestaan. In een machtiging moet staan bij wie de gegevens worden opgevraagd en om welke gegevens het gaat. De machtiging kan slechts betrekking hebben op een specifiek geval en mag dus niet algemeen worden geformuleerd. Een werkzoekende moet de machtikging vrijwillig tekenen. Een machtiging mag niet gekoppeld zijn aan een formulier dat de werkzoekende verplicht moet invullen. Dit wekt namelijk de indruk dat de werkzoekende ook verplicht is om de machtiging te tekenen.

Bestandsvergelijking

Er zijn verschillende vormen van bestandsvergelijking: de wettelijk verplichte en de niet wettelijk verplichte (themacontroles). Bij wet is geregeld dat het inlichtingenbureau (IB) de bestanden van een aantal organisaties binnen de keten van werk en inkomen met elkaar vergelijkt. Is ergens sprake van overlap, dan stuurt het IB een samenloopsignaal naar de organisatie die hier belang bij heeft. Deze organisatie zoekt het signaal uit en onderneemt zo nodig actie richting werkzoekende. Bij bestandsvergelijkingen in het kader van themacontroles zijn er twee varianten: de geanonimiseerde bestandsvergelijking en de vergelijking waaruit tot het individu herleidbare gegevens voortkomen.
Geanonimiseerde bestandsvergelijkingen kunnen statistisch materiaal opleveren over bepaalde risicofactoren. Deze gegevens kunnen worden gebruikt voor het opstellen van een risicoprofiel. Over geanonimiseerde bestandsvergelijkingen hoeft de werkzoekende niet te worden geïnformeerd. Voorwaarde is wel dat de gegevens op geen enkele manier te herleiden zijn (of zullen worden) tot individuele personen. De Participatiewet staat het vergelijken van bestanden met de daar genoemde organisaties toe, mits voldaan is aan een aantal criteria. Zo moet de bestandsvergelijking noodzakelijk zijn voor een goede uitvoering van de Participatiewet. Verder moet bestandsvergelijking niet een te zwaar middel zijn in verhouding tot het doel dat men wil bereiken (het proportionaliteitsbeginsel). Ook moet het doel niet op een andere wijze, die minder belastend is voor de persoonlijke levenssfeer, kunnen worden bereikt. Dit is het zogenoemde subsidiariteitsbeginsel.

Het ontvangen van tips

Nadat een tip is binnengekomen, beoordeelt de gemeente of deze mag worden verwerkt. Alleen rechtmatig verkregen tips mogen worden verwerkt. De gemeente heeft de plicht om de werkzoekende op de hoogte te stellen van het feit dat zij informatie over hem heeft verkregen. Op grond van de Wbp is het mogelijk om de informatieplicht op te schorten in het belang van het onderzoek. De werkzoekende moet na afloop van het onderzoek alsnog worden geïnformeerd over de met de tip verkregen gegevens en de wijze waarop het onderzoek heeft plaatsgevonden. Deze verplichting geldt ongeacht het resultaat van het onderzoek. De werkzoekende wordt dus ook geïnformeerd over een onderzoek dat geen fraude aan het licht heeft gebracht.

d) Boek 1 Burgerlijk Wetboek
Hierin zijn diverse bepalingen opgenomen over het door de rechter opleggen en het door gecertificeerde instellingen uitvoeren van kinderbeschermingsmaatregelen. Verschaffen van inlichtingen aan Raad voor de Kinderbescherming. Wie die op grond van de wet, ambt of beroep tot geheimhouding is verplicht, kan zonder toestemming van degene die het betreft, aan de Raad voor de Kinderbescherming inlichtingen verschaffen, als dit noodzakelijk is voor de uitoefening van de taken van de raad.

e) Algemene wet bestuursrecht: ambtgeheim

Hierin is een bepaling opgenomen die geheimhouding oplegt aan iedereen die betrokken is bij de uitvoering van de taak van een bestuursorgaan ten aanzien van 'gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden'. Dat geldt ook voor de instellingen en de daarvoor werkzame personen die een bestuursorgaan inschakelt of die een bij of krachtens de wet toegekende taak uitoefenen. Ook andere wetten verwijzen naar dit ambtsgeheim, zoals de Wet bescherming persoonsgegevens en het Wetboek van strafvordering.

f) Wet publieke gezondheid: meldingsplicht infectieziekten, dossierplicht jeugdgezondheidszorg

Hierin is een meldingsplicht geregeld voor bepaalde besmettelijke ziekten (artsen mogen de hierop betrekking hebbende persoonsgegevens zonder toestemming van de betrokkene verstrekken). Het is ook verplicht om voor de uitvoering van de jeugdgezondheidszorg een digitaal bestand bij te houden.

g) Wet op de beroepen in de individuele gezondheidszorg (Wet BIG): titelbescherming, tuchtrechtspraak, medisch beroepsgeheim

Deze wet gaat over de kwaliteit van de beroepsuitoefening, met onder meer bepalingen over titelbescherming en tuchtrechtspraak. Tevens is in deze wet de plicht opgenomen om 'geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim ter kennis van hem is gekomen of wat daarbij ter kennis is gekomen en waarvan hij het vertrouwelijke karakter had moeten begrijpen'.

h) Wet bescherming persoonsgegevens (Wbp): doelbinding, informatieplicht, privacy rechten

Geeft, ter uitvoering van artikel 10 van de Grondwet, aanvullende regels voor gebruik van persoonsgegevens om het recht op bescherming van de persoonlijke levenssfeer te waarborgen. Doelbinding, transparantie (uitgewerkt in informatieplicht en privacy rechten), proportionaliteit en subsidiariteit zijn hierbij kernbegrippen.

i) Wet geneeskundige behandelingsovereenkomst (Wgbo): geheimhoudingspicht, dossierplicht, positie wilsonbekwamen

Deze wet is van toepassing op handelingen met betrekking tot de geneeskunst. Geeft bepalingen met betrekking tot geheimhoudingsplicht, dossierplicht, positie meerderjarige wilsonbekwame patiënten en minderjarigen. Wat betreft verwerking van persoonsgegevens zijn er kleine verschillen tussen Wgbo en de Wbp, waarbij de Wgbo, als lex specialis, voorgaat voor zover toepassing van beide wetten strijdigheid zou opleveren. DeWgbo geeft de patiënt het recht om een aanvulling in het dossier op te nemen (in Wgb is alleen het recht opgenomen om onjuiste gegevens te corrigeren), kent een ongeclausuleerd vernietigingsrecht (in Wbp is verwijderingsrecht wel aan voorwaarden gebonden) en kent een bewaartermijn van vijftien jaar (Wbp kent geen vaste bewaartermijn, maar zegt wel dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is).

j) Wet politiegegevens: incidentele en structurele verstrekkingen door politie

De Wet politiegegevens kent een gesloten verstrekkingensysteem. Dat wil zeggen dat limitatief is benoemd aan wie de politie in het kader van de taakuitoefening gegevens mag verstrekken (dit is uitgewerkt in het Besluit politiegegevens). Op degenen die deze gegevens vervolgens ontvangen, rust een eveneens in deze wet geregelde geheimhoudingsplicht die een verbijzondering is ten opzichte van de algemene geheimhoudingsplicht in de Awb en de Wbp. Uitzondering op deze geheimhoudingsplicht is er als de wet dat voorschrijft of de gegevens noodzakelijk zijn om een taak uit te voeren. In het kader van de Jeugdwet kan de gemeente bijvoorbeeld gegevens van de politie ontvangen over gedragingen van een jeugdige en deze delen met de Raad voor de Kinderbescherming en gecertificeerde instellingen met het oog op de voorbereiding van kinderbeschermingsmaatregelen of jeugdreclassering.

Is de verstrekking niet expliciet benoemd, dan kunnen in bijzondere gevallen - voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en in overeenstemming met het bevoegd gezag politiegegevens incidenteel worden verstrekt aan personen of instanties voor de volgende doeleinden:

- het voorkomen en opsporen van strafbare feiten;
- het handhaven van de openbare orde;
- het verlenen van hulp aan hen die deze behoeven;
- het uitoefenen van toezicht op het naleven van regelgeving.

Dat kan ook structureel zijn, indien dit voor een samenwerkingsverband is van de politie met personen en instanties. In dat geval worden extra eisen gesteld aan de vastlegging van de daarop betrekking hebbende beslissing. Bij incidentele verstrekkingen moet men denken aan crisisachtige situaties, bijvoorbeeld bij een KIZ-aanpak (Kleinschalige Incidenten of Zedenzaken). Bij structurele meldingen gaat het altijd om verstrekkingen die via een convenant/reglement zijn vastgelegd. Denk bijvoorbeeld aan de aanpak van veelplegers in het kader van het Veiligheidshuis of aan de aanpak van jeugdoverlast in het kader van een wijkgerichte, sluitende aanpak.

k) Wet justitiële en strafvorderlijke gegevens: verstrekkingen strafvorderlijke gegevens door het Openbaar Ministerie

Deze wet stelt regels met betrekking tot de verwerking van justitiële gegevens in persoonsdossiers en de verklaring omtrent het gedrag. Regelt onder andere dat het College van procureurs-generaal (namens het Openbaar Ministerie) strafvorderlijke gegevens kan verstrekken aan personen of instanties (met name de burgemeester) voor de volgende doeleinden:

- het voorkomen en opsporen van strafbare feiten;
- het handhaven van de orde en veiligheid;
- het uitoefenen van toezicht op het naleven van regelgeving;
- het nemen van een bestuursrechtelijke beslissing;
- het beoordelen van de noodzaak tot het treffen van een rechtspositionele of tuchtrechtelijke maatregel;
- het verlenen van hulp aan slachtoffers en anderen die bij een strafbaar feit betrokken zijn;
- het verrichten van een privaatrechtelijke rechtshandeling door een persoon of instantie die met een publieke taak is belast.

Die verstrekking moet noodzakelijk zijn met het oog op een zwaarwegend belang of de vaststelling, de uitoefening of de verdediging van een recht in rechte. Bovendien moet redelijkerwijs worden voorkomen dat de gegevens herleidbaar zijn tot een ander dan betrokkene. Veel verstrekkingen aan de burgemeester met het oog op orde en veiligheid vallen hieronder, bijvoorbeeld ook in verband met zijn taakuitoefening in het kader van de Wet tijdelijk huisverbod.

l) Wetboek van strafvordering: verschoningsrecht

De wet biedt getuigen in een rechtszaak, die gebonden zijn aan een geheimhoudingsplicht op grond van een ambts- of beroepsgeheim, de mogelijkheid om zich te verschonen, te weigeren een antwoord te geven. Ook kan het zijn dat om die reden de in de wet geregelde aangifteplicht niet geldt. Het is aan de rechter om te bepalen of en in welke mate het verschoningsrecht van toepassing is, wat neerkomt op een belangenafweging.

m) Wet gemeentelijke schuldhulpverlening: identificatieplicht en uitwisseling gegevens

Deze wet ondersteunt bij het vinden van een adequate oplossing die gericht is op de aflossing van schulden, indien redelijkerwijs is te voorzien dat een natuurlijk persoon niet zal kunnen voortgaan met het betalen van zijn schulden of indien hij in de toestand verkeert dat hij heeft opgehouden te betalen. De wet regelt ook de nazorg. Voor een goede werking van de wet zal sprake zijn van informatie-uitwisseling. De betrokkene moet zich bij aanmelding in het kader van deze wet legitimeren. Voor een integraal overheidsoptreden ten aanzien van de voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten, wordt samengewerkt door de colleges van burgemeester en wethouders, het Uitvoeringsinstituut werknemersverzekeringen en de Sociale verzekeringsbank.

n) Wet basisregistratie personen: verstrekkingen aan andere overheidsorganen en derden

Deze wet vormt het algemeen kader voor de uitvoering van de zogenaamde 'basisregistratie personen' door de overheid (BRP was voorheen GBA:gemeentelijke basisadministratie). Geregeld is onder meer in welke gevallen de gemeente gegevens uit deze registratie mag verstrekken aan andere overheidsorganen of derden. In het kader van deze wet kan onder bepaalde voorwaarden toegang worden verleend tot (delen) van de basisregistratie.

0) Wet algemene bepalingen Burgerservicenummer / Wet gebruik Burgerservicenummer in de zorg: gebruik Burgerservicenummer

Deze wetten verplichten de overheid en zorgaanbieders om bij hun taakuitoefening gebruik te maken van Burgerservicenummers. Ook is hierin een legitimatieplicht geregeld. Dat moet zorgen voor minder

fouten bij gegevensuitwisseling, voorkomen van persoonsverwisseling, eenvoudiger declareren en betere bescherming tegen identiteitsfraude.

Bijlage 3: Privacy Matrix
[Bijlage 3 is aan de linkerkant te downloaden.]